ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

A Distributed Publisher Driven Secure Data Sharing Scheme for Information Centric Iot

[1] Ch.Tishitha, [2] N.Kesava Rao, [3] M.Anupa, [4] A.Jyothsna, [5] K.Mounika
[1][2][3][4] Narayana Engineering College, Gudur

Abstract: This paper presents a critical review of Failure Modes and Effect Analysis (FMEA). Although the method is almost 70 years old, in literature there are still many researchers, both from academy and industry, devoted to improve it and overcoming unsolved and still open problems. The aim of this work consists in analysing a representative pool of scientific papers (220) and patents (109), in order to have an overview of the evolution of the method and try to understand if the efforts spent to improve it effectively answer to the several criticisms found in literature. All documents have been classified according to authors, source, and four technical classes dealing with the applicability of the method, representation of the cause and effect chain, risk analysis and integration with the problem-solving phase. A detailed analysis of the results allowed us to identify the most current problems, the improvement paths, and which other methods and tool are proposed to be integrated with FMEA.

Index Terms— FMEA, FMECA, Risk Analysis, Patents

IoT (Internet of Things) is likely to have a major impact on human lives as new services and applications are developed through integration of the physical and digital worlds. It is predicted that 50 billion devices will be connected through IoT by 2020, and vast amounts of data will be generated from those devices. Today, most IoT services are designed based on Internet technology [2], which was originally conceived for end-to-end communications. Based on such technology, IoT data sharing applications have been developed on the basis of centralized servers/clouds, which produce redundant and duplicate tra_c and bring out large latencies. Such a considerable volume of redundant Ruidong Li (corresponding author) and Hitoshi Asaeda are with the Network System Research Institute, National Institute of Information and Communications Technology, With regard to the use of IoT applications, users are usually concerned only about the IoT data that they retrieve rather than where the data are stored or cached . Information-Centric Networking (ICN) is an emerging technology that enables users to retrieve data from close caches without the need to access distant servers or clouds each time. Reducing the redundant tra_c overhead and data retrieval latency by moving data from clouds to caches close to users is a promising approach. It integrates computing power and storage to alleviate the bottleneck of network bandwidth resources [5]. Among the existing ICNs, Content-Centric Network (CCN)/Named Data Network (NDN) [6][9] is one of the most promising architectures; therefore, in this paper, we focus on CCN/NDN.

Compared to Internet-based IoT designs, ICN-based IoT designs have several salient and distinctive features with regard to security, heterogeneity, fast configuration, and diverse communication paradigms [10-16][19], besides a reduction in tra_c and latency. ICN is expected to be one of the fundamental technologies that will support IoT applications and services in the future, and for simplicity, hereafter, we refer to the IoT designs using ICN as ICIoT. ICIoTs have recently been widely discussed for use in IoT applications, such as smart cities , smart grid [16], smart home [14], IoT data sharing [11], serviceoriented architectures [13], and data collection in IoT [15]. The design requirements and challenges as well as the applicability of ICIoT have also been discussed in IRTF ICNRG [12]. ICIoT has emerged as a promising solution to provide viable IoT services to users [11][12][19]. To realize a true IoT vision, ensuring security.

To address this issue, we propose a Distributed Publisherdriven secure Data sharing for ICIoT (DPD-ICIoT) to enable IoT data to be securely shared based on publisherdefined policy. DPD-ICIoT provides flexible authorization from publishers to users. In DPD-ICIoT, CP-ABE is employed to provide flexible authorization from publishers to users. To balance centralized management and distributed retrievals for attributes, attribute manifest (AM) and data manifest (DM) are introduced and distributedly cached in the network. Thus, publishers can retrieve AMs from close copyholders instead of the centralized attribute servers. Herein, AM and DM are the data chunks, with the type of "Manifest", that describe attributes and data, respectively. Further, to reduce the large tra_c overhead of attribute updates, we propose an Automatic Attribute Self-update Mechanism (AASM) to enable the update of attributes without

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

querying the distant server. Compared with the existing CP-ABE scheme, the total bandwidth cost in packet transmissions consumed for attribute retrievals can be greatly reduced.

The main contributions of this paper are as follows. (1) To the best of our knowledge, this is the first work to investigate publisher-driven fine-grained access control in a ubiquitously distributed caching scenario for ICIoT. We integrate CP-ABE with the typical ICN, CCN/NDN [6][9], and propose a novel DPD-ICIoT scheme for providing distributed, secure, and flexible data sharing for ICIoT. (2) We employ a key chain mechanism for e_cient data encryption and decryption. (3) We design the AM to enable the close copy retrievals of attributes and propose an AASM to provide e_cient attribute update. (4) System evaluation is performed to compare the proposed DPD-ICIoT scheme with the existing CP-ABE scheme.

THREATS AND SECURITY REQUIREMENTS

In this section, we detail the threats and security requirements for a typical IoT use scenario. Threats should be inhibited from an architectural level and IoT data should be only accessible for a specific set of Users irrespective of where it is cached. The threats often occur when a Publisher publishes IoT data, or an immediate node caches data, or a User retrieves data. They can be mainly classified as impersonation attacks and man-in-the-middle attacks (MIMAs).

An impersonation attack can be defined as using an impersonated identity for malicious/selfish purposes. In the attack A4 in Fig. 1, the attacker impersonates P3 to publish the data. In attack A1 in Fig. 1, the attacker impersonates U1B to retrieve data from the cloud. For MIMA, the data, which are published by a Publisher and cached in routers, access points, BSs, or servers, can be retrieved from the network, and illegally modified by the attackers during transmissions or at caches. Attack A5 is to illegally modify the data when they are retrieved from P2 by U3; attack A3 is to illegally modify the data when they are cached at a BS at Domainb; attack A2 is to illegally modify the data when they are retrieved from the network by U2. Besides these attacks, the Publishers need to restrict the capability of Users to retrieve the data they publish.

With the existing CP-ABE scheme, all the attribute values and attribute updates need to be provided through centralized servers, such as attribute server and DSAs. In contrast, the attribute values are described in AMs and retrieved from close caches. Herein, we perform system evaluations to compare the existing CP-ABE scheme with the proposed DPD-ICIoT scheme. We consider that the metric for comparison is the ratio between the bandwidth cost of the DPD-ICIoT scheme at the lowest performance situation with at most one cached copy in one domain and the bandwidth cost for CP-ABE. The bandwidth cost is defined as the bandwidth consumption for communications. Assume that the network is divided into many domains. In each domain, one piece of AM or DM or data chunk can only be cached at most once, which is the lowest performance for CCN. If more AMs are cached, the cost for AM retrieval will be reduced further. CCN is utilized as the method for data retrieval.

Let l be the average physical hops for one node to send packet to another node in one domain, and L be the average number of hops to send packets from one domain to another domain. The packet size is assumed to be PS Type. That is, Interest size is PS Interest, and AM packet size is S AM.To transmit one packet in one domain, the bandwidth cost consumed for transmission is l _ PS Type.

It is assumed that g denotes the total number of cached induplicate attributes in the entire network. We assume each attribute is associated with one AM. Let f be the average number of copies for each AM. It is assumed that the attributes are averagely updated R times during the period that one Publisher uses it, and each data can only be cached at most once in one domain. We assume T to be the average retrieval times for one piece of AM in a period by di_erent Publishers. Let pL be the probability for intra-domain AM retrieval when a AM request occurs. The inter-domain AM retrieval occurs with the probability 1 □ pL. We assumed that AASM can be used throughout the period in the DPDICIoT scheme. That is, after AM is retrieved, Publishers do not need to retrieve it from the network again. The notations for performance analysis are summarized in Table II. The objective is to model the bandwidth cost for AM retrievals in the proposed network in a period. The total cost consumed during a period equals to the sum of the cost consumed in AM retrieval procedures.

CONCLUSIONS

To march toward secure IoT data sharing, we investigated the IoT data sharing problem with regard to unauthorized access, illegal modifications, and impersonation attack, when IoT data are cached in a distributed manner in the

network. The contributions in this paper are summarized as follows.

We provided system descriptions and identified the security requirements for a typical IoT data sharing scenario in distributed caching environment. We proposed a novel DPD-ICIoT scheme to enable secure and flexible access control for IoT data, which absorbs the merits from both CP-ABE and CCN. The DPD-ICIoT scheme employs a key chain mechanism to provide e_cient cryptographic operations. The AM and DM are introduced in DPDICIoT, which are disseminated in the network for fast attribute and data retrieval. Coupled with this design, we proposed AASM to realize the automatic attribute update in a distributed manner. Moreover, system evaluations have been performed, which show that the DPD-ICIoT scheme can greatly reduce the bandwidth cost of attribute retrieval compared to existing server-based CP-ABE. There are several issues to be addressed in realizing secure IoT data sharing, such as trust management and IoT data life control. In the near future, we intend to integrate trust-based relations into IoT data provision to advance the current research a step further.

REFERENCES

[1] O. Vermesan, and P. Friess (Editors), "Internet of Things: Converging Technologies for Smart Enviroments and Integrated Ecosystems," River Publishers, 2013.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies,
Protocols and Applications," IEEE Communications Surveys & Tutorials, issue 99, June 2015.

[3] J. Granjal, E. Monteiro, and J. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, issue 3, pp.1294- 1312, Jan. 2015.

[4] D. Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group white paper, Apr. 2011. [5] H. Yin, Y. Jiang, C. Lin, Y. Luo, and